CLAIMS

What is claimed is:

Sub a1

1. A stream cipher comprising:

a first and a second data bit generator to generate in parallel a first and a second stream of data bits; and

a combiner function coupled to the first and second data bit generators, having a shuffle unit including a storage structure, to generate a pseudo random sequence by modifying the first stream of data bits with at least a stochastic stream of past values of the first stream of data bits generated by using the second stream of data bits to stochastically operate the storage structure of the shuffle unit to memorize and reproduce past values of the first stream.

2. The stream cipher of claim 1, wherein the combiner function generates the past values of the first stream of data bits by using the second stream of data bits to stochastically control writing of the first stream of data bits into storage locations of the storage structure, and at the same time, retrieving past written values from the storage locations being written into.

3. The stream cipher of claim 1, wherein at least one of the first and the second data bit generator comprises a linear feedback shift register.

4. The stream cipher of claim 1, wherein the storage structure comprises a memory unit having a plurality of addressable memory locations, an input port

coupled to the first data bit generator, an output port, at least one read address port and at least one write address port coupled to the second data bit generator.

5. The stream cipher of claim 1, wherein the combiner function comprises a 1 to n de-mutiplexor having an input bit line coupled to said first data bit generator, n output bit lines coupled to the storage structure, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1.

6. The stream cipher of claim 1, wherein the combiner function comprises an n to 1 mutiplexor having n output bit lines coupled to said storage structure, an output bit line, and at least one control bit line coupled to said second data bit generator, where n is an integer greater than 1.

7. The stream cipher of claim 1, wherein the stream cipher further comprises a third data bit generator coupled to the combiner function to generate a third stream of data bits for the combiner function, and the combiner function is to further operate the storage structure to memorize and reproduce past values of the first stream using the third stream of data bits.

8. The stream cipher of claim 7, wherein the stream cipher further comprises a fourth data bit generator coupled to the combiner function to generate a fourth stream of data bits for the combiner function, and the combiner function is to further operate the storage structure to memorize and reproduce past values of the first stream using the fourth stream of data bits.

9. The stream cipher of claim 1, wherein the combiner function further comprises a XOR function coupled to the first bit data generator and the storage unit to generate the pseudo random sequence by performing an XOR function on at least said first stream and its past values.

10. A method comprising:

generating in parallel a first and a second stream of data bits;

stochastically generating a stream of past values of the first stream of data bits using the second stream of data bits; and

generating a pseudo random sequence by combining the first stream of data bits with at least the stochastically generated stream of past values of the first stream.

11. The method of claim 10, wherein said stochastic generation of a stream of past values of the first stream of data bits comprises selectively writing the first stream of data bits into a plurality of storage locations based at least in part on said second streams of data bits, and at the same time, retrieving past written values of the first stream of data bits from the storage locations being written into.

12. The method of claim 10, wherein said generation of first and second streams of data bits comprises shifting a first and a second linear feedback shift register in parallel.

13. The method of claim 12, wherein the method further comprises initializing the first feedback shift register with a first plurality of key segments, and the second

linear feedback shift register with a second plurality of key segments and at least one initial vector segment.

14. The method of claim 10, wherein said stochastic generation of past values of the first stream of data bits comprises applying said first stream of data bits to an input port of the storage locations, and said second stream of data bits to a read and a write address port of the storage locations.

15. The method of claim 10, wherein said stochastic generation of past values of the first stream of data bits comprises applying said first stream of data bits to an input bit line of a 1 to n de-mutiplexor, and said second stream of data bits to a control bit line of the 1 to n de-multiplexor.

16. The method of claim 10, wherein said stochastic generation of past values of the first stream of data bits comprises applying said second stream of data bits to a control bit line of a n to 1 multiplexor.

17. The method of claim 10, wherein said generation of first and second streams of data bits further comprises generating a third stream of data bits, and said stochastic generation of past values of the first stream of data bits further uses said third stream of data bits.

18. The method of claim 17, wherein said generation of first and second streams of data bits further comprises generating a fourth stream of data bits, and said stochastic generation of past values of the first stream of data bits further uses said fourth stream of data bits.

19. The method of claim 10, wherein the method further comprises performing an XOR function on said first stream of data bits and at least its past values.

20. An apparatus comprising:

first and second data bit generation means for generating in parallel a first and a second stream of data bits; and

combiner means coupled to the first and second data bit generation means, including shuffling means having storage means, for generating a pseudo random sequence, by combining the first stream of data bits with at least a stochastically generated stream of past values of the first stream of data bits generated by using the second streams of data bits to stochastically operate the storage means of the shuffle means to memorize and reproduce past values of the first stream.

21. The apparatus of claim 20, wherein the combiner means uses the second streams of data bits to stochastically control writing of the first data streams into storage locations of the storage means, and at the same time, retrieving past values written into storage locations being written into.